学校编码：10384　　分类号_____密级_____

学号：X2010230691　　UDC_____

厦门大学

工 程 硕 士 学 位 论 文

普通发票网络服务系统的分析与设计

Analysis and Design of Invoice Network Service System

段旭初

指 导 教 师： 王 备 战 教 授

专 业 名 称： 软 件 工 程

论文提交日期： 2012 年 10 月

论文答辩日期： 2012 年 11 月

学位授予日期： 年 月

答辩委员会主席：_____

评 阅 人：

2012 年 月

厦门大学学位论文原创性声明

本人呈交的学位论文是本人在导师指导下，独立完成的研究成果。本人在论文写作中参考其他个人或集体已经发表的研究成果，均在文中以适当方式明确标明，并符合法律规范和《厦门大学研究生学术活动规范（试行）》。

另外，该学位论文为（　　）课题（组）的研究成果，获得（　　）课题（组）经费或实验室的资助，在（　　）实验室完成。（请在以上括号内填写课题或课题组负责人或实验室名称，未有此项声明内容的，可以不作特别声明。）

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人同意厦门大学根据《中华人民共和国学位条例暂行实施办法》等规定保留和使用此学位论文，并向主管部门或其指定机构送交学位论文（包括纸质版和电子版），允许学位论文进入厦门大学图书馆及其数据库被查阅、借阅。本人同意厦门大学将学位论文加入全国博士、硕士学位论文共建单位数据库进行检索，将学位论文的标题和摘要汇编出版，采用影印、缩印或者其它方式合理复制学位论文。

本学位论文属于：

（　　）1.经厦门大学保密委员会审查核定的保密学位论文，于　　年　　月　　日解密，解密后适用上述授权。

（　　）2.不保密，适用上述授权。

（请在以上相应括号内打“√”或填上相应内容。保密学位论文应是已经厦门大学保密委员会审定过的学位论文，未经厦门大学保密委员会审定的学位论文均为公开学位论文。此声明栏不填写的，默认为公开学位论文，均适用上述授权。）

声明人（签名）：

年　　月　　日

摘 要

普通发票网络服务系统是税务部门适应税务信息化的发展，利用信息技术加强和规范普通发票管理，以杜绝虚假发票和大头小尾票、堵塞税收漏洞的重要手段。该系统采用省级集中方式向纳税人提供网上开票服务，以便税务部门及时获取纳税人开具普通发票的真实信息。系统的终端用户涉及到数十万纳税人，每年的开票量数以亿计，发票数据中蕴含大量的纳税人商业机密，如何在保障信息安全的前提下为纳税人提供高效可靠的服务，成为系统推行成败的关键因素。系统在设计时必须综合权衡安全和服务的关系，对系统架构进行合理选型，安全架构合理设计，充分考虑特殊情况的处理。

论文首先介绍了普通发票网络服务系统的开发背景和涉及到的一些技术和概念。其次对系统进行了需求分析以及系统的性能要求、安全要求和特殊情况的处理分析。接着介绍了系统的设计，包括系统的设计原则、应用蓝图、应用架构、功能架构、技术架构和部署架构，重点介绍了系统关键部分的设计，包括离线开票、接口设计、加密设计、性能设计和网络拓扑等服务端的安全设计。最后，对系统运行效果进行了总结并展望了系统在移动计算方面进行功能扩充的前景。

关键词：普通发票；开票服务；网络服务

Abstract

The implementation of Invoice Network Service System (INSS) is an important method of Tax Bureau to strengthen and standardize the ordinary invoice management, and prevent false invoices and irregular writing invoices, and eliminate the loopholes of taxation management. The system uses provincial centralized mode to provide taxpayers online invoicing services, so that the Tax Bureau can timely get the true information of taxpayers' invoicing. The users of INSS relate to hundreds of thousands of taxpayers whose confidential business information will be contained in the hundreds of millions of invoices which produced by INSS in each year. How to provide them with efficient and reliable services and guarantee the security of their confidential business information is the key factor of the success in the implementation of INSS. The design of INSS is a tradeoff between security and efficient services, which is built by a reasonable selection of system structure and security architecture and special case handling.

Firstly, the dissertation introduces the background of INSS and a number of relevant conceptions and techniques. Secondly, it introduces the system analysis, including the function requirements, system performance requirements, security requirements and the treatments of the special conditions. Then it introduces the system design, including design principle, application architecture, functional architecture, technical architecture and deployment architecture, off-line billing, design of interface, design of performance, design of encryption, network topology and the design of the Server safety. Finally, it summaries the system running effect and the prospect of the system's function expanding in mobile computing.

Keywords: Invoice; Invoicing Service; Network Service

目 录

第一章 引言 1

1.1 研究背景 1

1.2 论文的主要工作 1

1.3 论文的结构安排 2

第二章 相关技术 4

2.1 网络信息安全 4

2.1.1 公钥加密 4

2.1.2 对称加密 4

2.1.3 数字签名 5

2.1.4 数字证书 5

2.1.5 PKI 5

2.2 网络安全设备 7

2.2.1 防火墙 7

2.2.2 网闸 8

2.2.3 入侵检测系统（IDS） 8

2.2.4 入侵防御系统（IPS） 10

2.3 Oracle 数据库 11

2.4 架构模式 12

2.4.1 核心架构模式 12

2.4.2 Weblogic Server 12

2.4.3 Struts 框架 13

2.4.4 iBATIS 框架 13

2.4.5 OPOA 模式 14

2.4.6 AJAX 模式 15

2.4.7 MVC 模式 16

2.4.8 DAO 模式 17

2.4.9 AOP 模式.....18
2.5 本章小结.....18
第三章 系统分析.....19
3.1 功能要求.....20
3.2 性能要求.....21
3.3 安全要求.....21
3.3.1 管理级安全.....22
3.3.2 系统级安全.....22
3.3.3 数据输入输出控制.....23
3.3.4 数据审计与跟踪.....23
3.3.5 日志监控.....23
3.4 特殊情况处理.....23
3.5 本章小结.....25
第四章 系统设计.....26
4.1 系统设计原则.....26
4.2 总体应用.....28
4.3 应用架构.....29
4.4 系统技术架构.....31
4.4.1 系统技术架构选择.....31
4.4.2 技术实现架构.....32
4.4.3 组件库架构.....33
4.4.4 系统集成架构.....35
4.5 系统部署架构.....35
4.6 系统详细设计.....36
4.6.1 离线开票功能.....36
4.6.2 接口设计.....47
4.6.3 安全设计.....47
4.6.4 网络安全.....49
4.6.5 性能优化与设计.....50

4.6.6 设备运行环境.....52
4.7 本章小结.....53
第五章 总结与展望.....54
5.1 总结.....54
5.2 展望.....55
参考文献.....56
致 谢.....58

Contents

Chapter 1 Introduction....1

1.1 Research Background....1

1.2 Main Research Contents....1

1.3 Outline of the Dissertation....2

Chapter 2 Related Technologies....4

2.1 Network Information Security....4

2.1.1 Public Key Encryption....4

2.1.2 Symmetric Encryption....4

2.1.3 Digital Signature....5

2.1.4 Digital Certificate....5

2.1.5 PKI....5

2.2 Network Security Devices....7

2.2.1 Fire Wall....7

2.2.2 Network-Gap....8

2.2.3 Intrusion Detection System....8

2.2.4 Intrusion Prevention System....10

2.3 Oracle....11

2.4 Architecture Pattern....12

2.4.1 Core Framework....12

2.4.2 Weblogic Server....12

2.4.3 Struts Framework....13

2.4.4 iBATIS Framework....13

2.4.5 OPOA....14

2.4.6 AJAX....15

2.4.7 MVC....16

2.4.8 DAO....17

2.4.9 AOP....18

2.5 Summary....18

Chapter 3 System Analysis 19

3.1 Function Requirements 20

3.2 Performance Requirements 21

3.3 Security of System 21

3.3.1 Security of Management 22

3.3.2 Security of System 22

3.3.3 Data Input/Output Controlling 23

3.3.4 Data Auditing & Tracking 23

3.3.5 Logging 23

3.4 Treatments for the Special Conditions 23

3.5 Summary 25

Chapter 4 System Design 26

4.1 The Principles of Design 26

4.2 Overall Application 28

4.3 Application Architecture 29

4.4 Technical Architecture 31

4.4.1 The Technical Architecture of INSS 31

4.4.2 The Implementation of Technical Architecture 32

4.4.3 Component Libraries 33

4.4.4 System Integration 35

4.5 The Architecture of Deployment 35

4.6 The Detailed Design of the System 36

4.6.1 Offline Invoicing 36

4.6.2 Design of Interface 47

4.6.3 Design of Security 47

4.6.4 Security of Network 49

4.6.5 Performance Tunning 50

4.6.6 Running Environment 52

4.7 Summary 53

Chapter 5 Conclusions and Prospect 54

5.1 Conclusions 54

5.2 Prospect 55

References 56

Acknowledgements.....58

第一章 引言

1.1 研究背景

根据国家税务总局关于“简并票种、统一票样、建立平台、网络开具”的工作要求，为切实解决现行普通发票管理模式的弊端，有效加强税源控管手段和打击非法使用发票行为，不断健全发票管理制度体系，全面由“以票控税”转向“信息管税”的模式，网上开具普通发票的需求提到日程。

按照国家税务总局关于建立发票管理长效机制的要求，以“省级集中、统筹规划、逐步推广、技术先进、突出重点、注重实效、逐步完善”的指导原则，建立全省统一的发票网上开具系统，以加强税源的控制，提高发票管理的质效，打击、防范假发票和非法代开发票，突出发票信息采集的全面性、实时性，为税源监控以及税收管理提供实时、完整的信息；突出税务机关管理措施的及时性和有效性；突出发票信息的权威性，为公安、财政、审计等部门以及广大财务人员共同打击“供需两个市场”，切实提高防堵假发票的能力，实现发票开具全过程信息的通查，为实现案发地税务机关开展异地发票鉴定提供可能，从而降低公安机关假发票鉴定成本。最终为开票部门和税务管理机关提供一个方便、快捷、高效的发票管理平台。

1.2 论文的主要工作

普通发票网络服务系统作为税务机关提供给纳税人使用的服务系统，能否为纳税人所接受，取决于系统能否安全、可靠地提供服务。论文主要从系统的总体设计、安全设计和特殊情况的处理等方面来保证系统的安全、可靠服务。

系统总体设计遵循税务信息系统的设计标准和国际上应用成熟的总体架构设计理念以及其设计原则，同时参考了类似系统的成功经验。从体系架构、设计原则、平台选型、应用架构、功能架构、技术架构、系统部署、关键技术等方面制定设计约束和规则。系统在实现上体现了以架构模式、分层设计和组件化的思路和原则。作为网上办税服务厅的组成部分，在架构选型上遵循 J2EE 规范，在交互控制层采用简洁高效的异步通讯 AJAX 技术，服务层采用具有分布式运算能力的 EJB 组件，持久层采用基于 ORM 映射的 iBATIS 框架，在界面操作风格上采用和纳税人熟悉的车购税系统、专用发票远程认证系统相同的风格，并且可以

在网上办税服务厅框架下实现单点登陆，方便了企业的操作。

为了确保纳税人敏感信息的安全，系统从系统登陆、数据传输、网络部署、权限分配等多方面考虑了系统的安全，主要体现在 CA 体系认证、管理体系设计、数据安全设计和网络安全设计：

1、CA 体系认证：利用 CA 系统进行身份认证，判别所有登录到网上发票开具系统的用户所具有的身份，包括没有证书、持有证书但不是一个有效证书（包括税务 CA 签发但已经失效的证书和非税务 CA 签发的证书）和持有合法证书的用户；资格认证：通过身份认证过程来提取出合法用户的证书甄别名 DN 与后台数据库里存储的纳税人信息映射表里进行匹配，来确认该用户在本系统的真实身份，所具有的操作权限，判定其在本系统中具备的资格。

2、管理体系设计：系统后台管理采用了与综合征管系统相同的权限体系结构，有用户、角色、岗位、模块组成的权限体系，实现对 5 级（超级管理员、省市县管理员、税局用户、企业管理员、开票员）用户管理，支持岗位灵活配置。

3、数据安全设计：传输控制加密采用采用 MD5 数据项加密、在传输过程中采用 SSL 加密通道，本地缓存数据采用嵌入式转码加密数据库。

4、网络安全设计：网络安全方面在某省局现有的纳税服务平台安全体系基础上增加安全设备的方式实现，在利用以往的安全经验的同时尽量减少对原有系统的影响。

系统通过互联网提供服务，网络的暂时中断不可避免，为了应对企业网络不稳定的情况，系统设计了应急开票功能。企业在网络联通的情况，自动下载发票的领购、分发信息，并可同步本地的商品信息和客户信息，发票开具过程中与本地数据库进行交互，开具的信息保存到本地，当在网络联通的情况下由系统自动上传开具的发票信息。不仅解决了应急开票的问题同时也减轻了开票过程中对服务器的压力。

1.3 论文的结构安排

论文共分五章，各章内容如下：

第一章是引言，主要介绍了普通发票网络服务系统的研究背景，简述论文的主要研究内容。

第二章介绍了普通发票网络服务系统在设计中所涉及的技术。

第三章对系统进行了分析，阐述了系统设计的重点。

第四章详细阐述了系统的总体设计、关键部分的详细设计。

第五章对系统的运行效果进行了总结，并对后续完善和移动计算的应用前景进行了展望。

第二章　相关技术

普通发票网络服务系统直接面向纳税人提供服务，所涉及的纳税人涵盖各行各业，开票数据蕴含诸多商业机密，因此系统对可靠性和安全性有较高的要求，既要保证信息安全又要确保系统能为纳税人提供高效系统服务。在系统设计中，需要从网络、数据库、安全体系、应用架构等各方面综合考虑。

2.1 网络信息安全

2.1.1 公钥加密

加密方案使秘密消息可以在不安全信道上进行传输，换句话说，加密方案为这些消息提供了保密性。在现代密码学中，主要有两类加密方案。一类称为对称密钥加密方案，其中消息发送者和接收者共享相同的秘密密钥。另一类称为非对称加密方案，该类方案可以在无密钥共享的条件下，实现消息的加密传输。在非对称加密中，加密密钥与解密密钥不同。因为加密密钥或者称为公钥是公开的，而解密密钥或者称为私钥是保密的，所以此类加密方案又被称为公钥加密[1]。公钥密码的概念最早由 Diffie 和 Hellman[2]提出。最早的具体公钥加密方案是由 Rivest,Shamir 和 Adleman[3]与 Merkle 和 Hellman[4]分别提出。

2.1.2 对称加密

在对称加密系统中[5]，通信双方必须拥有相同的密钥。如果发送方用密钥 k 和加密算法 C 将明文 m 加密成对应的密文 C_m，接收方必须用密钥 k 和解密算法 D 将密文 C_m 解密为对应的明文 m。

典型的对称加密算法，如 DES， AES[5]等，都满足上述计算规则。明文一般就是发推者传送的大家都理解的信息或有意义的信息，而密文则是表面上无规则，或没有实际意义的信息。攻击者如果没有密钥就无法从密文 C_m 获得明文 m 的任何信息。密文 C_m 的安全性取决于密钥的安全性而不是算法的安全性。

在对称加密系统中，密文可以通过不安全信道传输，然而密钥必须通过安全信道传送。否则一旦密钥被截获，通信双方的秘密就会被发现。密钥安全分配成为至关重要的问题。在对称加密系统中要求：①通信双方已经共享了一个密钥，而且这个密钥已经以某种安全的方式分配给他们；②需要一个密钥分配中心[6]。

对称加密系统的缺点：当涉及到多个用户之间的相互通讯时，密钥分配将成为制约对称密码应用的一个关键因素，如 n 用户相互通讯时，在没有 KDC（Key

Distribution Center：密钥分配中心）时，至少需要 $O(n^2)$的密钥量。因此当用户增加时，密钥空间急剧增大，必须考虑引入额外的密钥管理机制对密钥进行有效的管理和分发[7][8]。

2.1.3 数字签名

数字签名是一种电子签名，用于认证消息来源并保证消息在传输中没有被篡改。公钥数字签名的概念最早由 Diffie 和 Hellman[2][4]提出。具体的签名方案最早由 Rivest，Shamir 和 Adleman[3]提出。类似于公钥加密，公钥签名方案也有公钥和私钥。签名者使用私钥消息签名，任何人可用签名者公钥验证签名。因此，公钥/私钥也被称为验证密钥/签名密钥。由于公钥算法运算量巨大，效率低，采用公开密钥结合信息摘要(Message Digest，MD)的方法可以提高认证速度和效率。信息摘要能产生信息的数字“指纹”，其目的是为了确保信息没有被修改或变化，保证信息的完整性不被破坏[9]。

2.1.4 数字证书

数字证书 (Digital certificate)：是由认证权威 CA 发放并经其数字签名的，包含公开密钥拥有者以及公开密钥相关信息的一种数据结构，可以用来证明数字证书持有者的真实身份。数字证书是 PKI 体系中最基本的元素，PKI 系统所有的安全操作全部通过数字证书来实现[10][11]。

2.1.5 PKI

PKI 是“Public Key Infrastructure”的缩写，意为“公钥基础设施”。简单地说，PKI 就是利用公钥密码理论和技术建立的、提供信息安全服务的基础设施。公钥密码体制是目前应用最广泛的一种加密体制，在这一体制中，加密密钥与解密密钥各不相同，发送信息的人利用接收者的公钥发送加密信息，接收者再利用自己专有的私钥进行解密。这种方式既保证了信息的机密性，又能保证信息具有不可抵赖性。目前，公钥体制广泛地用于身份认证、数字签名和密钥交换等领域[12]。

PKI 的基本组成：PKI 在实际应用上是一套软硬件系统和安全策略及协议的集合。这个集合包括了认证权威 CA、注册机构 RA、资料库、PKI 策略、PKI 应用等[9][13]。

认证权威（CA）：为了确保用户的身份及他所持有密钥的正确匹配，公钥系统需要一个可信的第三方(Trusted Third Part，TTP)充当认证权威(Certification